

CONTINUATION IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Samantha Maxwell, a Special Agent with the Federal Bureau of Investigation, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I have been employed as a Special Agent (“SA”) of the Federal Bureau of Investigation (“FBI”) since July 2012, and am currently assigned to the Detroit Division, Grand Rapids Resident Agency. While employed by the FBI, I have investigated federal criminal violations related to firearms violations, to include felon in possession of firearms or ammunition, weapons of mass destruction, domestic terrorism, international terrorism, as well as crimes involving technology. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. My duties include the investigation of alleged violations of federal criminal laws, including matters involving violations of 18 U.S.C. § 922 (felon in possession of a firearm or ammunition) and its subsections.

3. The statements contained in this continuation are based in part on information provided by U.S. federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement officers; information gathered from investigative sources of information; and my experience, training, and background as a Special Agent.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The property to be searched is **(1) a Nokia cellular phone, Model: N152DL, S/N: A00000V590241527214, with IMEI 358205601714135,** also referred to as Device 1, and **(2) an Apple iWatch, S/N: A2477-W3RCK76MD6,** also referred to as Device 2, (collectively “Subject Devices”), and described in Attachment A. The **Subject Devices** are currently located at the Unites States Probation Office in Grand Rapids, Michigan.

6. The applied-for warrant would authorize the forensic examination of the **Subject Devices** for the purpose of identifying electronically stored data particularly described in Attachment B.

FACTUAL BACKGROUND OF INVESTIGATION

7. Beginning in 2018, Aaron FEIN was located at the Canadian border in Sault Ste. Marie, Michigan by Customs and Border Protection (CBP) with a notebook of schematics for building potentially explosive devices, specifically what were believed to be pipe bombs and remote triggering devices. Items in the notebook included notations regarding mechanical explosions and shrapnel flying at high rates of speed. Homeland Security Investigations (HSI) and Federal Bureau of Investigation (FBI) agents continued investigation of FEIN following the encounter with CBP.

8. During the 2018 investigation, FEIN was interviewed and his computer device(s) were searched. FEIN informed law enforcement agents that he spent a significant amount of time on the Internet and had an interest in mass shooters and empathy towards terrorists. Subsequent searches of his devices revealed search history including, but not limited to the following: numerous searches of “Tsarnaev” and variations of the Tsarnaev brother’s names who conducted the Boston Marathon Bombing, as well as various individuals convicted of bombing related to terrorist acts such as Timothy McVeigh, Ramzi Yousef, and Ted Kaczynski. Additional searches were located for “Introduction to the Technology of Explosives” and “Explosives Engineering Fundamentals,” and more.

9. During the investigation, FEIN began seeking out firearms and firearm components. He was ultimately prohibited from possessing any firearms or components by the State of Michigan pursuant to a court order. Despite this, FEIN actively sought to purchase firearms at multiple retailers in Michigan. Ultimately, FEIN was denied those purchases and began renting firearms to shoot at firearms ranges. Thereafter in 2019, FEIN left the state, traveling to a firearms range in Ohio. FEIN was questioned about this trip and admitted to talking to range employees about converting “80 percent lower” parts into a completed lower rifle assembly and how to assemble a semi-automatic rifle.

10. An additional search of FEIN’s residence in 2019 yielded gun parts, an AR-15 Lower Parts Kit, billet designs, jig, drill bits, and other parts to be used to manufacture firearms from 80% kits. Once again, law enforcement agents located notebooks with notes regarding explosives, as well as electrical components including wires, batteries, and circuit boards.

11. FEIN made materially false statements during his interview about his actions at the firearms range in Ohio, which ultimately led to his charge and conviction for violation of 18 U.S.C § 1001 in the Western District of Michigan. FEIN was sentenced in March 2020 to a period of incarceration to be followed by three years of post-release supervision. FEIN’s term of supervision is currently set to end in March 2024.

12. In April 2023, the Michigan Kent County Sheriff's Office (KCSO) identified FEIN as the subject of an unarmed robbery causing injury on April 24, 2023 at a Menards store in Comstock Park, Michigan. According to the KCSO, FEIN attempted to steal a 20-volt power cut-out tool and two packages of allergy medication from Menards. When store employee(s) confronted FEIN about the theft, FEIN allegedly fled and punched an employee in the face while exiting the store. The stolen cut-out tool was recovered. This power tool was consistent with a tool used to convert firearms kits and parts into functional firearms parts.

13. On May 17, 2023, the United States (US) Probation Office in the Western District of Michigan conducted a search of FEIN's home, pursuant to his supervised release conditions and based on the attempted theft of a tool used in the manufacture of firearms.

14. During the search several items were discovered related to the manufacture of firearms, to include functional firearms, components, ammunition – five .223 caliber live rounds, seventeen 9mm rounds, eighty five .22 caliber rounds, and seventy one 5.56 caliber live rounds – magazines, a drill press with metal shavings, lower receivers for rifles, lower receiver molds, firearms armory tools, circuit boards, batteries, notebooks containing notes about firearms, electrical power, and possible location data, and the **Subject Devices**. More specifically, one completed privately made firearm (PMF) pistol of an unknown manufacturer was

discovered. The Michigan State Police laboratory subsequently test fired this pistol and confirmed it to be a fully functioning firearm.

15. **Device 1** was located hidden inside the zippered compartment of a golf bag in the basement of FEIN's residence. **Device 2** was located hidden inside a box secreted inside a Cinnamon Toast Crunch cereal box inside FEIN's bedroom closet.

16. The **Subject Devices** are currently in the lawful possession of the US Probation Office following the search of FEIN's residence for violations of supervised release conditions. Therefore, while the US Probation Office might already have all necessary authority to examine the **Subject Devices**, I seek this additional warrant out of an abundance of caution to be certain that an examination of the **Subject Devices** will comply with the Fourth Amendment and other applicable laws.

17. In my training and experience, I know that the **Subject Devices** have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the **Subject Devices** first came into the possession of the US Probation Office.

TRAINING AND EXPERIENCE

18. Based on my training and experience, and information obtained from other agents with experience in federal firearms violations, I know that individuals who possess firearms often take pictures and videos of themselves and others with

firearms. These pictures are frequently taken with and stored on cellular phones or other digital devices. These pictures and videos are also frequently stored and/or posted on the public and private features of various social media platforms, to include Facebook, Twitter, and Instagram, among others. Individuals who unlawfully possess firearms frequently utilize cellular devices to access the internet, email, and various social media platforms, to include Facebook, Twitter, and Instagram, among others, to advertise and facilitate the sale and purchase of firearms.

19. Individuals who utilize various social media platforms, to include Facebook, Twitter, and Instagram, among others, often post pictures with the fruits of the criminal exploits, specifically individuals often post pictures of themselves and other with illegally obtained firearms. Furthermore, these individuals often utilize cellular phones to gain access to various social media platforms.

20. Individuals who utilize cellular phones, computers, tablets, other electronic communication devices, the internet, email, and various social media platforms, to include Facebook, Twitter, and Instagram, among others, knowingly or unknowingly leave a GPS footprint, including, but not limited to IP addresses of the device's location; the email account or social media account's location. Furthermore, these individuals often utilize cellular devices and social media platforms to post or tag themselves at various locations, as well as post or tag other

individuals with them. All of the above-referenced geographical location information can aid law enforcement in establishing a timeline, pinpoint the individual's location during criminal acts, and identify additional suspects.

21. Further, based on my knowledge of the 2018 investigation into FEIN, I am aware that FEIN by his own admissions frequently spends a significant time on the Internet and utilizes electronic devices to search for firearms-, explosion-, and terrorism-related subjects, including The Anarchist Cookbook and explosives technology. Based on the fact that both the **Subject Devices** are capable of accessing the Internet, as discussed in greater detail below in paragraphs 23 and 24, I believe there is probable cause to conclude that FEIN used the **Subject Devices** to perform similar searches and that evidence regarding his unlawful possession of firearms, ammunition, and other explosive components will be located on the **Subject Devices**. In addition, the fact that both **Subject Devices** were located in hidden locations, I believe that FEIN secreted these **Subject Devices** to prevent their detection by law enforcement agents. In my training and experience, subjects hide devices containing contraband—including evidence related to their unlawful possession of firearms and ammunition—to prevent their detection by law enforcement agents.

TECHNICAL TERMS

22. Based on my training, experience, and information obtained from other agents, I know the below statements are accurate and use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal

computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

23. Based on my training, experience, and research, and from consulting the manufacturer’s advertisements and product technical specifications available online at <https://support.tracfone.com> I know that **Device 1** has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

24. Based on my training, experience, and research, and from consulting the manufacturer’s advertisements and product technical specifications available

online at <https://apple.com> I know that **Device 2** has capabilities that allow it to serve as a wireless telephone, digital camera remote, portable media player, GPS navigation device, and PDA.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

25. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

26. There is probable cause to believe that things that were once stored on the mobile **Subject Devices** may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that digital files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, or mobile device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a mobile device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

27. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **Subject Devices** were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **Subject Devices** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary

to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

28. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

29. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

30. Some information stored within a computer, phone, or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or phone may both show a particular location and have geolocation information incorporated into its file data. Such file data also typically contains information indicating when the

file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user.

31. Information stored within a mobile device or phone may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information within the device may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

32. A person with appropriate familiarity with how a computer or phone works can, after examining this forensic evidence in its proper context, draw conclusions about how devices were used, the purpose of their use, who used them, and when.

33. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer and phone evidence is not always data

that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer or phone is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

34. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

35. Computer and phone users can attempt to conceal data within equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension .jpg often are image files. A user can easily change the extension to .txt to conceal the image and make it appear that the file contains text. Computer and phone users can also attempt to conceal data by using encryption. Encryption involves the use of a password or device, such as a dongle or keycard, to decrypt the data into readable form.

36. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit imaging, or otherwise copying the **Subject**

Devices and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium. This might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

37. I respectfully submit that there is probable cause to believe that AARON FEIN has violated 18 U.S.C. § 922(g) (felon in possession of firearm or ammunition). I submit that this application supplies probable cause for a search warrant authorizing the examination of the **Subject Devices** described in Attachment A to seek the items described in Attachment B.

38. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).